Über

Substitutionsfunktionen

modulo 11

und die

analytische Darstellung

der

Permutationen von 5, 7, 11 Elementen.

Inaugural-Dissertation

zur

Erlangung der philosophischen Doktorwürde

an der

Kgl. Friedrich-Alexander-Universität zu Erlangen

von

Franz Rinecker
Kgl. Reallehrer in Nürnberg.

Regensburg.
Verlag von Alfred Coppenrath.
1886.

Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41546420_0124

Über

Substitutionsfunktionen

modulo 11

und die

analytische Darstellung

der

Permutationen von 5, 7, 11 Elementen.

Inaugural-Dissertation

zur

Erlangung der philosophischen Doktorwürde

an der

Kgl. Friedrich-Alexander-Universität zu Erlangen

von

Franz Rinecker
Kgl. Reallehrer in Nürnberg.

Regensburg.
Verlag von Alfred Coppenrath.
1886.

I. Abschnitt.

§ 1.

Einleitung.

Hermite hat in den *Comptes rendus,* tome 57 pag. 750 uff. unter dem Titel: *Sur les fonctions de sept lettres* eine sehr interessante Arbeit über die Substitutionsfunktionen mod 5 u. 7 veröffentlicht und sind die von ihm gewonnenen Resultate, unter welchen das Kriterium der Substitutionsfunktionen von besonderer Bedeutung ist, unter anderen von *Camille Jordan,* in dessen Werk: *Traité des substitutions* etc. pag. 88—91 und ausführlicher in *Serret, cours d'algèbre supérieur* Bd. II p. 378 wiedergegeben worden.

Die vorliegende Abhandlung führt in ihrem I. Abschnitt die Untersuchungen über Substitutionsfunktionen auf den mod 11 weiter und zwar mit der Beschränkung, dass zunächst nur die ein-, zwei- und dreigliedrigen derselben abgeleitet sind, wobei für die zweigliedrigen Funktionen ein neues Kriterium zugrund gelegt ist.

Im Abschnitt II ist ein System conjugierter Funktionen gegeben, die analytische Darstellung der Permutationen von 5,7,11 Buchstaben mit Hilfe von Substistutionsfunktionen besprochen und die Möglichkeit dargethan, sämtliche Permutationen durch bezüglich 1,3,5 Funktionen einfachster Art (formes réduites) mittelst Iteration von gegebenen Fundamentalsubstitutionen zu entwickeln. Der Weg, welcher eingeschlagen wurde, um zum vorgesteckten Ziele zu gelangen, ist, meines

Wissens, neu, und die Resultate, welche sich in der Folge ergaben, dürften der Art sein, dass durch die Bekanntgabe derselben der Wissenschaft immerhin ein Dienst geleistet wird.

Für die Anregung und die jederzeit bereitwillige Unterstützung, welche ich durch Herrn Professor Dr. Paul Gordan bei der Bearbeitung der vorliegenden Schrift erfuhr, sage ich demselben auch an dieser Stelle meinen besten Dank.

§ 2.

Analytische Darstellung der Substitutionen.

Ist eine beliebige Permutation von n Elementen A_0 gegeben und man geht von dieser zu einer anderen A_1 derselben Elemente über, so bezeichnet man die Operation durch $\binom{A_1}{A_0}$ und nennt den Übergang eine Substitution.*)

Analytisch betrachtet kann man die Elemente durch einen einzigen Buchstaben mit veränderlichem Index x z. B. a_x darstellen, wo x der obigen Zahl entsprechend n verschiedene Werte annimmt. Eine Permutation hat dann die Form $a_0 a_1 a_2 a_3 \cdots a_{n-1}$. Existiert eine Funktion von x z. B. f(x), welche auch die n Werte des Index nur in anderer Reihe gibt, so vollzieht man eine Substitution, indem man f(x) statt x in obigem a_x setzt. Sind speziell die n Elemente die Zahlen 0,1,2, $\cdots$ (n—1), so fallen die Buchstaben mit den Indices zusammen und man hat als analytischen Ausdruck der ersten Permutation die Grösse x. Jede Funktion f(x), welche mod (n)**) ein System von n incongruenten Zahlen liefert, also ein vollständiges Restsystem hat, wird statt x gesetzt eine Substitution bewirken und nennen wir Funktionen dieser Art Substitutionsfunktionen.

Über Ausdrücke, welche zu Substitutionen geeignet sind, kann man im Allgemeinen aus *Dirichlet Zahlentheorie* § 21 und 26 folgern, dass die einfachsten davon (formes réduites) Polynome mit ganzen Koëffizienten, die kleiner als der Mo-

*) Serret, cours d'algèbre, Bd. II, N. 404, 474.

**) Der Modul ist stets als Primzahl aufzufassen.

dul sind und unter welchen der Koëffizient des ersten Gliedes 1 ist, sein werden. Zugleich kann die zweithöchste Potenz sowohl, als auch die Konstante als irrelevant bezeichnet werden. Letztere kann das Restsystem des übrigen Teiles nur gleichmässig verändern, d. h. alle Reste nehmen um dieselbe Grösse zu, weshalb aus gleichen Resten wieder gleiche hervorgehen. Erstere verschwindet durch die cyklische Substitution $(\frac{x+1}{x})$.

Wir können somit sagen: die einfachsten Funktionen, welche Substitutionen vollziehen, sind im Allgemeinen von der Form:

$$f(x) = x^{\nu} + ax^{\nu-2} + bx^{\nu-3} + \cdots mx$$

§ 3.

Potenzen.

Die Anzahl aller nten Potenzreste ist nach Dirichlet Zahlentheorie § 31 $= (p-1):\delta$, wo δ den grössten gemeinschaftlichen Teiler der Zahlen n und $p-1$ bezeichnet. (p Modul).

Sollen die Reste, wie hier nötig, sämtlich inkongruent sein, so muss $\delta = 1$, d. h. n und $p-1$ müssen relative Primzahlen sein.

Für den Modul 11 erhält man somit folgende Potenzen (eingliedrige Funktionen), welche volle Restsysteme geben und deshalb zu Substitutionen passend sind:

$$x^3, \quad x^7, \quad x^9.$$

§ 4.

Allgemeine Ableitung von Substitutionsfunktionen; Grad derselben.

In § 2 wurde der allgemeinste Ausdruck einer Substitutionsfunktion und zwar in reduzierter Form angeschrieben. Es heisst:

$$f(x) = x^{\nu} + ax^{\nu-2} + bx^{\nu-3} + \cdots mx$$

Wie gross ist „ν“ und was sind die Koëfficienten; diese Fragen sind nunmehr zu beantworten.

Da nach dem Fermat'schen Satze $x^{p-1} \equiv 1\ (p)$ also $x^p \equiv x$, so vermutet man, dass sobald eine ganze Funktion p^{ten} Grades mit ganzzahligen Koëfficienten ein volles Restsystem hat, dasselbe auch für jene Funktion $p-2^{ten}$ Grades statt habe, welche man aus der ersten erhält, indem man die Glieder x^p und mx vereinigt und das ax^{p-1} als Konstante wegstreicht. Der Grad der Funktionen reduzierter Form könnte demnach p—2 nicht übersteigen.

In der That werden wir diesen bekannten Satz auch durch die allgemeine Ableitung der Substitutionsfunktionen bestätigt finden.

Das allgemeine Mittel zur Aufstellung der Substitutionsfunktionen ist die *Lagrange'sche Interpolationsformel*, denn es handelt sich zunächst um eine Funktion $p-1^{ten}$ Grades, von welcher man p Werte kennt.

Hermite findet mit Benützung der Interpolationsformel, wie sie Cauchy*) gibt,

$$\begin{aligned}\Theta(x) = a &- x(b + 2^{p-2}c + \cdots (p-1)^{p-2}k)\\ &- x^2(b + 2^{p-3}c + \cdots (p-1)^{p-3}k)\\ &\vdots\\ &- x^{p-2}(b + 2c + \cdots (p-1)k)\end{aligned}$$

welche Form sich auch bei Serret findet.

Man kann aber auch einen anderen Weg gehen, indem man die Interpolationsformel mit der Partialbruchentwickelung in Verbindung bringt. Es ist:

$$\frac{f(x)}{\varphi(x)} = \frac{f(\alpha)}{(x-\alpha)\varphi'\alpha} + \frac{f(\beta)}{(x-\beta)\varphi'\beta} + \cdots$$

wobei $\varphi(x) = (x-\alpha)(x-\beta)\cdots$

Multipliziert man beiderseits mit $\varphi(x)$ so hat man:

$$f(x) = (x-\beta)(x-\gamma)\cdots(x-\mu)\frac{f(\alpha)}{\varphi'(\alpha)} + (x-\alpha)(x-\gamma)\cdots\frac{f(\beta)}{\varphi'(\beta)} + \cdots$$

ein Ausdruck, welcher für $x = \alpha$ den Wert $f(\alpha)$, für $x = \beta$ den Wert $f(\beta)$ etc. annimmt. Diese $f(\alpha)$, $f(\beta)\cdots$ sind die

*) Cauchy, Lehrbuch der algebraischen Analysis, deutsch von Sulzer Cap. 3, und Cap. 4 § 1 und V. Note.

gegebenen Funktionalwerte, $\alpha,\beta\cdots$ die der Variabelen und f(x) ist in der Lagrange'schen Interpolationsformel dargestellt.

f(x) vereinfacht sich noch durch folgende Überlegung wesentlich:

$$\text{Es ist } \alpha,\ \beta,\ \gamma \quad = 0,\ 1,\ 2,\ 3\cdots\cdot\ (p-1)$$
$$\text{also } \varphi(x) = x(x-i)(x-2)\cdots(x-p+1)$$
$$\equiv x^p - x$$
$$\varphi'(x) = px^{p-1} - 1$$
$$\equiv -1 \text{ wegen } x^{p-1} \equiv 1$$

mithin sind sämtliche Nenner $\equiv -1$. Ferner:

$$(x-\alpha)(x-\gamma)\cdots(x-\mu) \equiv x^{p-1} - 1$$

$$(x-\alpha)(x-\gamma)(x-\delta)\cdots(x-\mu) = x(x-2)(x-3)\cdots(x-(p-1))$$
$$\equiv \frac{x^p - x}{x-1} = x^{p-1} + x^{p-2} + x^{p-3}\cdots x$$

aber $(x-1)^{p-1} = x^{p-1} - \binom{p-1}{1}x^{p-2} + \binom{p-1}{2}x^{p-3} - \cdots\cdot 1$ (p ungerade)

$$\equiv x^{p-1} + x^{p-2} + x^{p-3} + \cdots 1$$

da $\binom{p-1}{\nu} \equiv \pm 1$ je nachdem ν gerade oder ungerade, denn

$$\binom{p-1}{\nu} = \frac{(p-1)(p-2)(p-3)\cdots(p-\nu)}{1.\quad 2.\quad 3.\qquad \nu}$$
$$\equiv \frac{-1.-2.-3.\quad -\nu}{1.\quad 2.\quad 3.\qquad \nu} \equiv \pm 1$$

also:

$$(x-\alpha)(x-\gamma)\cdots(x-\mu) = x(x-2)(x-3)\cdots(x-(p-1))$$
$$\equiv (x-1)^{p-1} - 1$$

Ähnlich:

$$(x-\alpha)(x-\beta)(x-\delta)\cdots(x-\mu) \equiv (x-2)^{p-1} - 1$$

Unter Berücksichtigung der obigen Kongruenzen ist nunmehr $f(x) \equiv f(\alpha) - x^{p-1} f(\alpha) + f(\beta) - (x-1)^{p-1} f(\gamma) + \cdots\cdot$ und da nach der Voraussetzung, wenn $f(\alpha) \equiv a$, $f(\beta) \equiv b$ etc. gesetzt wird, die Grössen a, b, c$\cdots$eine Permutation der Zahlen $0, 1, 2\cdots(p-1)$ bilden, so hat man $a + b + c + \cdots \equiv 0$

und $f(x) = -x^{p-1}\cdot a - (x-1)^{p-1} b - \cdots\cdot$; oder $-a \equiv \xi_0$ etc.

$$f(x) = x^{p-1}\xi_0 + (x-1)^{p-1}\xi_1 + \cdots\cdot$$

Setzt man nun für x die Werte $0, 1, 2\cdots$ so bekommt man folgende Gleichungen:

$$f(0) = \xi_1 + \xi_2 + \xi_3 \cdots = s - \xi_0 \equiv -\xi_0$$
$$f(1) = \xi_0 + \xi_2 + \cdots = s - \xi_1 \equiv -\xi_1$$
$$\vdots \qquad \vdots \qquad \vdots$$
$$f(p-1) = \xi_0 + \xi_1 + \xi_2 \cdots = s - \xi_{p-1} \equiv -\xi_{p-1}$$

wodurch ein System von p Gleichungen gegeben ist, aus welchem man zu f die ξ und umgekehrt berechnen kann. Man erkennt, dass die ξ_0, ξ_1 etc. die Ergänzungen der vorgelegten Funktionalreste auf den Modul in der Reihenfolge f(0), f(1) etc. sein müssen, sobald zu einer Permutation die zugehörige Funktion gesucht wird. Die abgeleitete Funktion lässt sich mithin kurz anschreiben:

$$f(x) \equiv \Sigma \xi_\nu (x - \nu)^{p-1}$$
$$\equiv \Sigma \xi_\nu (x^{p-1} + \nu x^{p-2} + \nu^2 x^{p-3} + \cdots \nu^{p-1})$$

und da sich hieraus für x^{p-1} der Koëfficient $\Sigma \xi_\nu = \xi_0 + \xi_1 + \cdots \equiv 0$ ergibt, so ersieht man, dass die Funktion, welche einem ganz beliebig gewählten Restsystem zugehört, den Grad p—2 nicht übersteigt.

Beispiel. Es soll eine Funktion berechnet werden, welche modulo 7 das Restsystem 3,6,5,4,2,1,0 hat.

Setzt man $\xi_0 = 4$, $\xi_1 = 1$, $\xi_2 = 2$, etc. also die Ergänzungen der obigen Reste auf 7 so wird:

$$f(x) \equiv \Sigma \xi_\nu (x - \nu)^{p-1} \equiv (1+4+2+6+2)x^5 + (1+1+6+3+3)x^4$$
$$+ (1+2+4+5+1)x^3 + (1+4+5+6+5)x^2$$
$$+ (1+1+1+3+4)x + (1+2+3+5+6)$$
$$\equiv x^5 + 6x^3 + 3x + 3$$

Die ersten 3 Glieder dieser Funktion bilden eine der formes réduites, welche Hermite in $x^5 + ax^3 + 3a^2x$ (a beliebig) zusammengefasst hat, wenn man a=6 nimmt.

Wir können schliesslich behaupten, dass die einfachsten ganzen Funktionen mit ganzen Koëfficienten, welche Restsysteme haben, für den Modul p die Form annehmen:

$$f(x) = x^{p-2} + ax^{p-4} + bx^{p-5} + \cdots mx$$

§ 5.

Über das Hermite'sche Kriterium der Substitutionsfunktionen.

Legt man die im vorhergehenden Paragraphen von Hermite angegebene Form

$$\Theta(x) = a - x\,(b + 2^{p-2}c + \cdots (p-1)^{p-2}k) - \cdots$$

zu Grund, so lautet das Kriterium:

$$\sum_{x=0}^{x=p-2} \Theta^n(x) \equiv 0 \pmod{p}$$

woraus man schliessen kann, dass bei $\Theta(x)$ in jeder Potenz, nachdem mittelst $x^{p-1} = 1$ reduziert ist, die Summe der durch Reduktion erhaltenen Konstanten kongruent Null ist.

Da die Richtigkeit dieses Kriteriums nicht nur von *Hermite,* sondern auch und zwar in etwas anderer Art von *Serret* (n° 464) und endlich wieder anders von *Camille Jordan* (n° 115 pag 89) bewiesen ist, so könnten wir füglich eine eingehendere Besprechung unterlassen, wenn uns nicht die Berichtigung eines Irrtums im erstgenannten Beweise nötigte, das Kriterium noch genauer zu untersuchen.

Hermite sagt nämlich:

Formons la suite des puissances $\Theta^2(x)$, $\Theta^3(x) \cdots \Theta^{p-2}(x)$, et soit, en général,

$$\Theta^n(x) = (n)_0 + (n)_1\, x + (n)_2 x^2 \cdots (n)_n x^{n\,(p-2)},$$

je dis, qu'on aura

$$(n)_0 + (n)_{p-1} + n_{2\,(p-1)} \cdots (n)_{(n-1)\,(p-1)} \equiv 0$$

effectivement, a, b, $\cdots$ k représentant dans un ordre quelconque un système de résidus, on a:

$$\begin{aligned}\Theta^n(0) + \Theta^n(1) + \cdots \Theta^n(p-1) &= a^n + b^n + \cdots k^n \\ &\equiv 1^n + 2^n \cdots k^n \\ &\equiv 0 \pmod{p}\end{aligned}$$

de sorte qu'en éliminant dans $\Theta^n(x)$ les puissances de x dont l'exposant est supérieur à p—1, à l'aide de la relation $x^{p-1} = 1$, le coefficient du terme indépendant auquel on sera ainsi amené devra être congru à zéro.

Der Irrtum besteht in der ersten Kongruenz. Es sollte heissen $(n)_0 + (n)_{(p-1)} + \cdots \equiv a^n$ oder

$$(n)_{(p-1)} + (n)_{2\,(p-1)} + \cdots \equiv 0$$

denn $(n)_0$ ist nichts Anderes als a^n oder $\Theta^n(0)$ vor der Reduktion mittelst $x^{p-1} \equiv 1$. Diese Ueberlegung führte mich zu folgender Darstellung des Kriteriums. Ist $f(x)$ eine reduzierte Form (§ 2), so hat man:

$f(0) = 0$; $f^n(0) = 0$
$f^n(x) \equiv \varphi(x) + C$ [nach Reduktion
$f^n(0) \equiv \varphi(0) + C$ mittelst $x^{p-1} \equiv 1$]
$\therefore 0 \equiv C$

also unmittelbar: die Summe der durch Reduktion erhaltenen Konstanten in $f^n(x)$*) ist stets $\equiv 0$.

Ist $f(x)$ eine allgemeine Form, so wird:
$f(0) = a$; $f^n(0) = a^n$
$f^n(x) \equiv \varphi(x) + a^n + C$ (nach Reduktion)
$f^n(0) = a^n + C$
$a^n = a^n + C$
$0 \equiv C$ wobei C wieder die Summe der durch Reduktion erhaltenen Konstanten.

Ich glaube nun dadurch, dass ich nicht die ganze Summe sondern nur das eine Glied $\Theta^n(0)$ untersucht habe, die Bedingung $C \equiv 0$, worauf ja hier Alles ankommt, besonders deutlich begründet zu haben, denn der Übergang ist eigentlich:
$\Sigma\,\Theta^n(x) \equiv \alpha + C + \beta + C + \gamma + C + \cdots$ (nach der Reduktion)
was $\equiv a^n + b^n + c^n + \cdots$ sein muss,
und zwar $\alpha + C \equiv a^n$; $\beta + C \equiv b^n$ etc.; die erste Kongruenz gibt $C \equiv 0$ wegen $\alpha = a^n$.

Beispiel:
$f(x) = x^6 + 2x$; Modulus 11.
$f(0) = 0$, $f^5(0) = 0$
$f^5(x) = x^{30} + 10x^{25} + 40x^{20} + 80x^{15} + 80x^{10} + 32x^5$
$\equiv x^5 + 11 \pmod{11}$
$f^5(0) \equiv 0 + 11$
$0 \equiv 11$; $C = 11 \equiv 0$.

*) $n < p-1$.

Aber

$$f(x) = 2 + 2x + x^6$$
$$f(0) = 2\ [a];\ f^5(0) = 2^5\ [a^n]$$
$$f^5(x) = \varphi(x) + 1 + 7 + 3 + 2^5$$
$$f^5(0) = 0 + 11 + 2^5$$
$$2^5 = 11 + 2^5\ [a^n = C + a^n]$$
$$0 = 11.$$

Auch die Betrachtung der Restsysteme führt auf die eben gegebene Ableitung.

Eine *forme réduite* hat ein Restsystem o, a, b, c $\cdots$, da $f(0) = 0$, also muss auch jede Potenz dieses Systems das Anfangslied „0“ haben, d. h. $f^n(0) = 0$ und das ist dann $C = 0$ oder bei den anderen Formen ist der erste Rest vielleicht „a“, dann ist die n^{te} Potenz a^n etc. $f^n(0) = a^n \equiv a^n + C$, $C \equiv 0$.

Die Kongruenz $(n)_0 + \cdots \equiv 0$ ist bei *Serret* und *Camille Jordan* nicht erwähnt, da sie, wie schon gesagt, andere Wege eingeschlagen haben.

So sagt *Serret:*

$$f(z) \equiv A_0 + A_1 z + \cdots A_{p-2}$$
$$[f(z)]^m \equiv f_m(z) \equiv A_0^m + A^m z + \cdots A_{p-1}^m z^{p-1} \pmod p$$

Posons en outre

$$(f(0))^m + (f(1))^m + \cdots = S_m$$

si l'on donne à z, les valeurs 0, 1, 2, $\cdots$ p—1 et qu'on ajoute les résultats, il viendra

$$S_m = -A_{p-1}^m$$

car z^{p-1} est congru à zéro ou à 1, suivant que z est nul ou différent de zéro, et la somme $1^\mu + 2^\mu + \cdots (p-1)^\mu$ est congrue à zéro si „μ“ est inférieur à p—1 u. s. w.

Schliesslich resultiert $A_{p-1}^m \equiv 0$.

Bei *Camille Jordan* ist:

$$(\varphi(x))^m \equiv A^{(m)} + A_1^{(m)} x + \cdots A_{p-1}^{(m)} x^{p-1} \pmod p$$

dann $\Sigma[\varphi(x)]^m \equiv pA_0^m + A_1^{(m)} \Sigma(x) + \cdots + A_{p-1}^{(m)} \Sigma x^{p-1}$

mais on a

$$\Sigma x \equiv \tfrac{(p-1)p}{2}\ ;\ \Sigma x^2 = \Sigma x\,(x+1) - \Sigma x$$
$$= \tfrac{(p-1)p(p+1)}{3} - \tfrac{(p+1)p}{2}$$

Donc Σx, $\Sigma x^2 \cdots \Sigma x^{p-2}$ sont divisibles par p; il en est de même de $\Sigma[\varphi(x)]^m$, dont les termes doivent être, à l'ordre près, ceux de Σx^m; enfin $\Sigma x^{p-1} \equiv p-1$; car x^{p-1} est nul si $x = 0$, et congru à 1 dans tous les autres cas : donc, en supprimant les multiples de p, la relation ci-dessus se réduira à $A_{p-1}^{(m)} \equiv 0$. —

Resultat wie bei *Serret*.

Das $pA_0^{(m)}$ in $\Sigma[\varphi(x)]^m$ ist interessant, insoferne dadurch die Unwichtigkeit der Konstanten $A_0^{(m)}$ oder n_0 in Bezug auf das Kriterium $\Sigma f^n(x) \equiv 0$ besonders klar zutage tritt.

Bei jeder Substitutionsfunktion gilt somit die charakteristische Eigenschaft $\Sigma f^n(x) \equiv 0$ und da auch umgekehrt in den angeführten Abhandlungen der Beweis geliefert ist, dass jede Funktion dann ein Restsystem besitzt, wenn für sie das gegebene Kriterium statt hat, so haben wir ein Mittel gewonnen, jede vorgelegte Funktion von der Form

$$f(x) = A + Bx + Cx^2 \cdots$$

daraufhin zu prüfen, ob sie ein Restsystem hat oder nicht. Wir sagen kurz, da es auf die Konstante nicht ankommt, so streichen wir zunächst in der zu untersuchenden Funktion die Konstante, wodurch die f(x) zu $\varphi(x)$ werden soll; alsdann ist f(x) eine Substitutionsfunktion, wenn nach der Reduktion mittelst $x^{p-1} = 1$ die $\varphi^n(0) \equiv 0$ ist, wobei $n = 2,3 \cdots p-2$.

Beispiel:

$f(x) = 3 + 4x^3 + 5x^7$ Mod. 13

$\varphi(x) = 4x^3 + 5x^7$

$\varphi^4(x) \equiv 9 + x^2 + 6x^4 + 7x^7 + x^8 + 11x^{11}$

$\varphi^4(0) \equiv 9$

mithin f(x) keine Substitutionsfunktion.

§ 6.

Die zweigliedrigen Substitutionsfunktionen.

Das im vorigen § entwickelte Merkmal der Substitutionsfunktionen setzt uns in den Stand für jeden Modul alle Funktionen mit Restsystem abzuleiten, wie dies auch von *Hermite* modulo 5 und 7 geschehen ist. Geht man jedoch auf andere Moduln über, so findet man sofort, dass die Po-

tenzierungen der mehrgliedrigen Funktionen viele Misslichkeiten in der Rechnung bereiten, weshalb es nahe liegt, die Funktionen nach der Anzahl ihrer Glieder einzuteilen und dann nach und nach von den zweigliedrigen aufsteigend die drei- und mehrgliedrigen zu bestimmen. Bei diesem Gang der Untersuchung ergab sich ein ganz wesentlich einfacheres Kriterium der zweigliedrigen Funktionen, als das im § 5 enthaltene, und ist es mit Hilfe desselben leicht möglich, für jeden Modul die zweigliedrigen Funktionen sofort so anzuschreiben, dass nur mehr ein Parameter berechnet werden muss.

Wir wollen nun in diesem § zuerst das Kriterium und die Bestimmung des Parameters im allgemeinen besprechen, um dann in § 7 die Funktionen speziell modulo 11 zu geben.

Bezeichnet man mit x irgend eine der Zahlen $0, 1, 2, 3, \cdots (p-1)$, so stellt μx, wenn „μ" die Zahlen der Reihe mit Ausschluss von 1 durchläuft, die Elemente der obigen Reihe ohne x vor.*) Somit sind x und μx zwei verschiedene Zahlen der Reihe $0, 1, 2 \cdots p-1$.

Ist nun $f(x) = x^m + ax^n$ zu untersuchen, so ersieht man, dass $x^m + ax^n$ nicht gleich $\mu^m x^m + a\mu^n x^n$ sein darf, also

$$x^m + ax^n - (\mu^m x^m + a\mu^n x^n) \gtrless 0$$
$$x^m(1-\mu^m) + ax^n(1-\mu^n) \gtrless 0$$
$$x^{m-n}(1-\mu^m) + a(1-\mu^n) \gtrless 0$$
$$x^{m-n} \gtrless -\frac{a(\mu^n-1)}{\mu^m-1}$$

Da nun $x^{m-n} \equiv -a\frac{\mu^n-1}{\mu^m-1}$ stets möglich gemacht werden kann, ausser wenn $m-n = \frac{p-1}{2}$ ist, so schliesst man:

Eine zweigliedrige Funktion ist geeignet, eine Substitution darzustellen, wenn die Exponentendifferenz der beiden die Funktion bildenden Potenzen $= \frac{p-1}{2}$ ist.

Wegen der Exponentendifferenz $\frac{p-1}{2}$ lässt sich nun bei den zweigliedrigen Funktionen als untere Grenze des Grades

*) Dirichlet, Zahlentheorie § 19.

„$\frac{p+1}{2}$“ sofort angeben, denn ist die niedrigere Potenz x, so ist die andere $x^{\frac{p+1}{2}}$. Die Funktionen liegen somit zwischen dem $\frac{p+1}{2}$ und p—2ten Grad.

Was endlich die Bestimmung des Parameters a in $f(x) \equiv x^m + ax^n$ anbelangt, so führt hier dieselbe Überlegung wie oben zum Ziele. Soll das Restsystem vollständig sein, so ist der Fall: $x^m + ax^n \equiv \lambda^m x^m + \lambda^n a x^n$ ausgeschlossen. Da $\lambda^{\frac{p-1}{2}} \equiv \pm 1$ je nachdem λ quadratischer Rest oder Nichtrest*), so kann man obige Gleichung reduzieren und endlich für a auflösen, wodurch man alle Werte erhält, welche der Parameter aus der Reihe $0, 1, 2 \cdots p-1$ nicht annehmen darf.

§ 7.

Die zweigliedrigen Substitutionsfunktionen modulo 11.

Nach § 6 handelt es sich nur um folgende 4 Funktionen:

$$\begin{aligned} f(x) &\equiv x^6 + ax \\ &\equiv x^7 + ax^2 \\ &\equiv x^8 + ax^3 \\ &\equiv x^9 + ax^4 \end{aligned}$$

Zur Berechnung von a hat man, sobald x und μx die ihnen im § 6 beigelegte Bedeutung haben, zu entscheiden, wann

$$f(x) \equiv f(\mu x) \text{ oder}$$
$$x^6 + ax \equiv \mu^6 x^6 + \mu a x.$$

Ist „x“ Rest, so wird „μx“ Rest oder Nichtrest je nachdem „μ“ R oder N R ist, im ersteren Falle hat man:

$$x + ax \equiv \mu x + \mu a x$$
$$\mu \equiv 1, \text{ was ausgeschlossen ist (§ 6).}$$

Im zweiten Falle wird:

$$x + ax \equiv -\mu x + \mu a x$$
$$1 + a \equiv -\mu + \mu a$$
$$a \equiv \frac{\mu + 1}{\mu - 1}$$

wobei $\mu \equiv 2, 6, 7, 8, 10$.

*) Dirichlet, Zahlentheorie § 33.

War also x Rest, so musste μx Nichtrest sein, weshalb sich für die Annahme x Nichtrest μx als Rest, also „μ“ auch Nichtrest ergeben hätte. Es wäre $-x + ax = \mu x + a\mu x$ und a wie oben. Aus $a = \frac{\mu+1}{\mu-1}$ folgt

$$a = 3;\ a = \tfrac{7}{5} \equiv 8;\ a = \tfrac{8}{6} \equiv 5;\ a = \tfrac{9}{7} \equiv 6.$$

Da ferner für $a = 1$

$$f(10) \equiv f(0) \equiv 0$$

und für $a = 10$

$$f(1) \equiv f(0) \equiv 0$$

ist, so hat man für a nur mehr die Werte 2, 4, 7, 9, so dass sich die Funktionen 6. Grades in der Form darstellen:

$$f(x) = x^6 \pm 2x \text{ und } f(x) = x^6 \pm 4x.$$

Macht man dieselbe Überlegung für die übrigen Funktionen, so wird zunächst

$$a = \frac{\mu^2+1}{\mu^2-1}$$

$$a = \tfrac{5}{3} \equiv 9;\ a = \tfrac{37}{35} \equiv 2;\ a = \tfrac{50}{48} \equiv 7;\ a = \tfrac{65}{63} \equiv 4$$

ferner

$$a = \frac{\mu^3+1}{\mu^3-1}$$

$$a = \tfrac{9}{7} \equiv 6;\ a = \tfrac{8}{6} \equiv 5;\ a = \tfrac{344}{342} \equiv 3;\ a = \tfrac{513}{511} \equiv 8$$

endlich

$$a = \frac{\mu^4+1}{\mu^4-1}$$

$$a = \tfrac{17}{15} \equiv 7;\ a = \tfrac{10}{8} \equiv 4;\ a = \tfrac{4}{2} \equiv 2;\ a = \tfrac{5}{3} \equiv 9$$

Hiemit ergeben sich folgende Funktionen:

$$f(x) = x^7 \pm 3x^2;\ x^7 \pm 5x^2$$
$$f(x) = x^8 \pm 2x^3;\ x^8 \pm 4x^3$$
$$f(x) = x^9 \pm 3x^4;\ x^9 \pm 5x^4$$

Die Binome 8. und 9. Grades können auch aus denen des 6. Grades abgeleitet werden, indem x durch x^3 bezüglich x^9 ersetzt, und das Binom mittelst $x^{10} \equiv 1$ reduziert wird.*) So erhält man z. B. aus $x^6 \pm 2x$.

---

*) Ähnliches gilt für die von *Hermite* angegebenen Funktionen (modulo 7), wenn man x durch x^5 ersetzt.

$$x^{54} \pm 2x^9 \equiv x^4 \pm 2x^9$$

$$x = \frac{y}{2}$$

$$\frac{y^4}{2^4} + \frac{2y^9}{2^9} \equiv 2^4 y^4 \pm y^9$$

$$\equiv y^9 \pm 5y^4 \text{ u. s. w.}$$

Unterscheidet man, wie *Hermite**) bei den Funktionen modulo 7, zwischen xR und NR so kann man die Binome auf Monome zurückführen. Es ist:

$$x^6 + 2x \equiv 3x \text{ (xR)}$$
$$\equiv x \text{ (NR)}$$

oder allgemein $x^6 + ax \equiv (a+1)x$, (xR)
$\equiv (a-1)x$, (xNR)

ähnlich $x^7 + ax \equiv (a+1)x^2$, (xR)
$\equiv (a-1)x^2$, (xNR)

also $x^m + ax^n \equiv (a+1)x^n$, (xR)
$\equiv (a-1)x^n$, (xNR)

wobei nach § 6: $m-n = \frac{p-1}{2}$.

Bevor wir das Kapitel von den zweigliedrigen Substitutionsfunktionen schliessen, wollen wir noch erwähnen, dass zwei Funktionen von der Art $x^m + ax^n$ und $x^m - ax^n$ umgekehrte Restsysteme haben, d. h. die Reste der einen geben in umgekehrter Ordnung die Reste der anderen. Diese Eigenschaft hängt mit dem Umstand zusammen, dass von den beiden Potenzen eines Binomes die eine von geradem die andere von ungeradem Grade ist.

Das Restsystem der ersteren Potenzen hat die Form:

0, 1, a, b, c, d, d, c, b, a, 1

das Restsystem von ungeraden Potenzen ist dagegen:

0, 1, m, n, p, q, −q, −p, −n, −m, −1

also z. B. $f(2) \equiv a$ im 1. Falle, dann ist $f(9) \equiv a$
$f(2) \equiv p$ „ 2. „ „ „ $f(9) \equiv -p$

mithin in $x^m + ax^n$ (m gerade, n ungerade angenommen)

---

*) Bei dieser Ableitung sollte es statt $x^4 + 3x \equiv 2x$ (xR) und $x^4 + 3x \equiv 4x$ (xNR), umgekehrt zuerst 4x und dann 2x heissen. Für Serret pag. 383 gilt dasselbe, da hier statt x nur z geschrieben ist.

$$f(3) \equiv b + \alpha \cdot n$$
$$f(8) \equiv b - \alpha \cdot n$$

oder in $f_1(x) = x^m - \alpha x^n$ wird

$$f_1(8) \equiv b + \alpha n$$

d. h. $f(3) \equiv f_1(8)$

Ähnlich für m ungerade und n gerade.

Beispiel:

$x^6 + 4x$ gibt die Reste: 0, 5, 6, 4, 9, 3, 7, 10, 2, 1, 8

$x^6 - 4x$ „ „ „ 0, 8, 1, 2, 10, 7, 3, 9, 4, 6, 5

Aus der Betrachtung des Restsystemes einer geraden Potenz ergibt sich sofort der Satz, welcher für jede Substitutionsfunktion von beliebiger Gliederanzahl gilt:

Die Glieder einer Substitutionsfunktion können niemals lauter gerade Potenzen der Variabeln sein, denn in diesem Falle ist $f(x) \equiv f(p-x) \pmod p$.

§ 8.

Die dreigliedrigen Substitutionsfunktionen mod 11.

Nach den Schlussbemerkungen des § 7 haben wir bei den Funktionen 6. Grades nur die folgenden zu untersuchen:

$$f(x) = x^6 + ax^4 + bx,$$
$$= x^6 + ax^4 + bx^3,$$
$$= x^6 + ax^3 + bx^2$$
$$= x^6 + ax^3 + bx$$
$$= x^6 + ax^2 + bx$$

Zunächst soll jedoch der Beweis dafür erbracht werden, dass eine Funktion niedrigeren Grades überhaupt nicht existiert.

Es kommen $f(x) = x^2 + ax$, $x^3 + ax$, $x^4 + ax^2 + bx$, $x^4 + bx$ und $x^5 + ax^3 + bx^2 + cx$, in Betracht.

Wir nehmen das Hilfsmittel von § 5 in unserer Darstellungsweise:

In der ersten Funktion ist $f^5(0) \equiv 1$, in der zweiten $f^4(0) \equiv 4a$, also $a = 0$; in der dritten $f^3(0) \equiv 3a$, $a = 0$; in

der vierten $f^5(0) \equiv 1$ und endlich in der fünften $f^2(0) \equiv 1$, so dass sämtliche Funktionen als unbrauchbar erwiesen sind.

Zu demselben Resultate gelangen wir in Bezug auf die obigen Funktionen 6. Grades, denn in den beiden ersten ist $f^2(0) \equiv 2a$, bei der dritten $f^3(0) \equiv 3b^2$; $b \equiv 0$, bei der vierten ist $f^3(0) \equiv 6\,ab$, also a oder b Null, die erstere Annahme gibt die Funktionen von § 7, und die letztere gäbe $x^6 + ax^3$, wofür die $f^5(0) \equiv 1$. In der letzten Funktion ist $f^3(0) \equiv 3a^2$; $a \equiv 0$. *Es existiert somit keine dreigliedrige Funktion 6. Grades.*

Bei den Funktionen 7. Grades sind folgende 10 Combinationen der Exponenten möglich, welche 10 zu untersuchenden Funktionen entsprechen:

1.) 7, 5, 4	5.) 7, 4, 3	8.) 7, 3, 2
2.) 7, 5, 3	6.) 7, 4, 2	9.) 7, 3, 1
3.) 7, 5, 2	7.) 7, 4, 1	10.) 7, 2, 1
4.) 7, 5, 1		

Da von nun an öfter höhere Potenzen von Trinomen zu bilden sind, welche bei den Exponenten 3, 4, 5, 6 bekanntlich 10, 15, 21, 28 Glieder liefern, so legen wir die allgemeine Form des polynomischen Lehrsatzes für $\alpha + \beta + \gamma$ zugrund und geben dann nur kurz in der Art $\alpha^2\beta\gamma^2$ etc. diejenigen Glieder an, welche nach der Reduktion von x^{10}, x^{20}, x^{30} Konstante geben. Wir gehen also aus von:

$$(\alpha + \beta + \gamma)^n = \Sigma \frac{n!}{\mu!\,\nu!\,\rho!}\,\alpha^\mu \beta^\nu \gamma^\rho$$

In den obigen 10 Funktionen gibt das Quadrat von 1, 3, 4 die Kongruenz $a^2 \equiv 0$, und jenes von 5—8, 9 die Kongruenzen $2b \equiv 0$ bezüglich $2a \equiv 0$, woraus $b \equiv 0$ oder $a \equiv 0$ folgt. Es bleiben sonach nur noch 4 Funktionen, denn sobald $a \equiv 0$, braucht man die übrigen Funktionen nicht mehr zu untersuchen, da die zweigliedrigen Funktionen im § 7 erledigt sind.

In der 6. Funktion ist $f^3(0) \equiv 3a^2b$ und bei Nr. 10 ist $f^3(0) \equiv 6\,ab$, indem die Glieder $\beta^2\gamma$ bezüglich $\alpha\beta\gamma$ die Konstanten liefern. In beiden Fällen hat man für $a \equiv 0$ die in § 7 bestimmten Binome, während $b \equiv 0$ keine Funktion gibt.

Schliesslich bleibt noch Nr. 2 und Nr. 7 zu untersuchen:

$$f^2(0) \equiv 2b + a^2 \equiv 0$$
$$f^4(0) \equiv 6b^2 + 12a^2b + a^4 \equiv 0$$

quadriert man die erste Gleichung und subtrahiert sie dann von der zweiten, so wird:

$$8a^2b + 2b^2 \equiv 0$$

also $b \equiv 0$ oder $4a^2 + b \equiv 0$ d. h. $b \equiv -4a^2 \equiv 7a^2$ und somit $15a^2 \equiv 0$, also $a \equiv 0$.

Bildet man noch die 6. Potenz, so geben die Glieder $\alpha^5\beta$, $\alpha^3\gamma^3$, $\alpha^2\beta^2\gamma^2$, $\alpha\beta^4\gamma$, β^6, $\beta\gamma^5$ Konstante. Man bekommt:

$$6a + 20b^3 + 90a^2b^2 + 30a^4b + a^6 + 6ab^5 \equiv 0$$

oder:

$$6a + 9b^3 + 2a^2b^2 + 8a^4b + a^6 + 6ab^5 \equiv 0$$

und durch $b \equiv 7a^2$

$$6a + 7a^6 + 10a^6 + a^6 + a^6 + 60a \equiv 0$$
$$11a + 8a^6 \equiv 0;\ 8a^6 \equiv 0$$

was wieder $a \equiv 0$ gibt und zur Kontrolle dienen kann.

In Nr. 7 endlich, also in $x^7 + ax^4 + bx$, worin die Differenz der aufeinanderfolgenden Exponenten 3 ist, gibt das Biquadrat durch die Glieder $\alpha\gamma^3$ und $\beta^2\gamma^2$ die Kongruenz:

$$4b^3 + 6a^2b^2 \equiv 0$$
$$b^2(2b + 3a^2) \equiv 0$$
$$b \equiv 0 \text{ oder } b \equiv \tfrac{-3}{2}\, a^2 \equiv 4a^2.$$

$b \equiv 0$ führt auf $a \equiv 0$, dagegen gibt $b \equiv 4a^2$ in die Kongruenz substituirt, welche der 5. Potenz angehört und welche durch β^5, $\alpha^2\beta\gamma^2$, $\alpha\beta^3\gamma$ Konstante hervorbringt, eine Identität.

Aus $a^5 + 8ab^2 + 9a^3b \equiv 0$
wird $a^5 + 7a^5 + 3a^5 \equiv 0$.

Von den dreigliedrigen Funktionen 7. Grades bleiben sonach nur diejenigen bestehen, welche der Form entsprechen:

$$f(x) \equiv x^7 + ax^4 + 4a^2x$$

worin $a \equiv 1, 2, 3 \cdots 10$ genommen werden darf.

Man wird im Folgenden sehen, dass die Substitution $x : x^9$ aus der eben abgeleiteten Funktion 7. Grades diejenige 9. Grades liefert, welche überhaupt allein möglich ist.

Wir gehen nun über zu den Funktionen 8. Grades.

Zu untersuchen sind hier 12 verschiedene Kombinationen:

1.) 8, 6, 5	4.) 8, 5, 4	8.) 8, 4, 3	10.) 8, 3, 2
2.) 8, 6, 3	5.) 8, 5, 3	9.) 8, 4, 1	11.) 8, 3, 1
3.) 8, 6, 1	6.) 8, 5, 2		12.) 8, 2, 1
	7.) 8, 5, 1		

Bei N 1 ist $f^2(0) \equiv b^2$; also $b \equiv 0$ dagegen geben die Quadrate von N 4, 5, 7 $a^2 \equiv 0$, dann von 10 die Kongruenz $2b \equiv 0$ von N 12 die $2a \equiv 0$.

Von N 2 gibt der Kubus: $3a^2 \equiv 0$.

„ N 3 „ das Biquadrat: $4a \equiv 0$.

Hiemit sind 8 von den 12 Funktionen beseitigt.

In N 6 gibt das Quadrat: $a^2 + 2b \equiv 0$

das Biquadrat: $a^4 + 12a^2b + 6b^2 \equiv 0$

$$8a^2b + 2b^2 \equiv 0$$

$$b(4a^2 + b) \equiv 0$$

mithin $b \equiv 0$ oder $b \equiv -7a^2$. Letzter Wert eingetragen:

$$a^2 + 14a^2 \equiv 0;$$

$$a \equiv 0$$

Der Kubus von N 8 gibt:

$$3a + 3ab^2 \equiv 0$$

$$a(1 + b^2) \equiv 0$$

$a \equiv 0$ oder $b^2 \equiv -1 \equiv 10$, was nicht möglich, da 10 kein quadratischer Rest.

Das Biquadrat liefert auch zur Kontrolle $4a^3 \equiv 0$.

In N 9 gibt der Kubus: $a + b^2 \equiv 0$

„ das Biquadrat: $4a^3 + 6a^2b^2 \equiv 0$

$b^2 \equiv 10a$ und in die zweite Kongruenz substituirt:

$$4a^3 + 5a^3 \equiv 0$$

$$a \equiv 0$$

Es erledigt noch N 11:

Kubus: $a^2 + 2ab \equiv 0$

Biquadrat: $12ab + 4a^3b \equiv 0$.

Die zweite Kongruenz ist erfüllt für $b \equiv 0$, für welchen Wert die erste auch $a \equiv 0$ gibt. In der That ist auch der andere Wert für a aus der 2. Kongruenz unbrauchbar, denn $3 + a^2 \equiv 0$, $a^2 \equiv -3$ ist nicht auflösbar. Ebenso erhält man in der 6. Potenz durch $\alpha^2\gamma^4$ und $\beta^2\gamma^4$ die nur für $a \equiv 0$ und $b \equiv 0$ giltige Kongruenz:

$$4b^4 + 4a^2b^4 \equiv 0$$
$$4b^4(1 + a^2) \equiv 0$$

Hiemit haben wir die Reihe der dreigliedrigen Funktionen 8. Grades erschöpft und dabei das nämliche negative Resultat wie für die des 6. Grades erhalten.

In Bezug auf die Funktionen des 9. Grades haben wir 21 Kombinationen durchzuprüfen.

1.) 9,7,6	7.) 9,6,5	12.) 9,5,4	16.) 9,4,3	19.) 9,3,2	21.) 9,2,1
2.) 9,7,5	8.) 9,6,4	13.) 9,5,3	17.) 9,4,2	20.) 9,3,1	
3.) 9,7,4	9.) 9,6,3	14.) 9,5,2	18.) 9,4,1		
4.) 9,7,3	10.) 9,6,2	15.) 9,5,1			
5.) 9,7,2	11.) 9,6,1				
6.) 9,7,1					

Die Quadrate von N 2 und N 7 führen auf $b^2 \equiv 0$, jene von N 4 und 8 auf $2ab \equiv 0$, von N 12, 13, 14 auf $a^2 \equiv 0$, von N 6, 11, 18, 20, 21 auf $2b \equiv 0$, womit noch 9 Funktionen restieren.

Der	Kubus	von N 1	gibt	$3a^2b \equiv 0$
„	„	„ N 3	„	$6ab \equiv 0$
„	„	„ N 5, 19	„	$3b \equiv 0$
„	„	„ N 16	„	$3ab^2 \equiv 0$
das	Biquadrat	„ N 17	„	$4ab^3 \equiv 0$

Sämtliche Kongruenzen bedingen für a oder b den Wert Null.

In N 15 führt das Quadrat und Biquadrat auf:

$$a^2 + 2b \equiv 0$$
$$\text{und } a^4 + 12a^2b + 6b^2 \equiv 0,$$

welche Kongruenzen wir oben bei N 8 der Funktionen 8. Grades behandelt haben.

In N 10 gibt der Kubus: $3b + 3ab^2 \equiv 0$
das Biquadrat: $6a^2 + 4a^3b \equiv 0$
oder $b(1 + ab) \equiv 0$
$a^2(3 + 2ab) \equiv 0$

Aus der ersten Gleichung folgt $b = 0$ oder $ab \equiv -1$, was in die zweite substituirt

$$a^2 \equiv 0 \text{ oder } a = 0 \text{ gibt.}$$

Schliesslich bleibt nur noch N 9, nämlich

$$x^9 + ax^6 + bx^3$$

bei welcher Funktion die Differenz der Exponenten wie vorher bei den Funktionen 7. Grades drei ist.

Bildet man die vierte und fünfte Potenz, wobei die Glieder $\alpha^3\gamma$, $\alpha^2\beta^2$ und bezüglich $\alpha^2\beta\gamma^2$, $\alpha\beta^3\gamma$, β^5 Konstante liefern, so hat man:

$$4b + 6a^2 \equiv 0$$
$$a(8b^2 + 9a^2b + a^4) \equiv 0$$
$$\text{d. h. } b \equiv -\tfrac{3}{2}\, a^2 \equiv 4a^2$$

und in 2 eingesetzt:

$$7a^4 + 3a^4 + a^4 \equiv 0$$

eine Identität.

Von den dreigliedrigen Funktionen haben sonach nur die folgenden beiden Formen Restsysteme: $x^7 + ax^4 + 4a^2x$ *und* $x^9 + ax^6 + 4a^2x^3$, *wobei die zweite, wie schon gesagt, aus der ersten mittelst* $x : x^9$ *erhalten wird.*

Für mod 7 sind die dreigliedrigen Funktionen in der Form $x^5 + ax^3 + 3a^2x$ (a beliebig) enthalten, welche eine bemerkenswerte Ähnlichkeit mit den obigen Formen aufweist.

II. Abschnitt.

Anwendungen.

§ 9.

Ableitung eines conjugierten Systemes.

Unter den in § 7 gegebenen zweigliedrigen Funktionen ist $x^9 + 3x^4$ eine Substitution der zweiten Ordnung und gibt Veranlassung zur Bildung eines conjugierten Systemes, d. h. *eines Systemes von Substitutionen, die ein- oder mehrmal mit einander oder mit sich selbst multipliziert wieder Substitutionen des Systemes geben.*)*

---

*) *Serret,* cours d'algèbre supérieur II. Bd. n° 412.

Es ist nämlich, wenn $x^9 + 3x^4 = \varphi(x)$ gesetzt wird:

$$\varphi(x)^9 + 3\varphi(x)^4 = x^6(x^5 + 3)^9 + 3x^6(x^5 + 3)^4$$
$$\equiv x^6(x^5+3)^4(x^{25}+4x^{20}+2x^{15}+6x^{10}+9x^5+1+3)$$
$$\equiv x^6(x^5+3)^5$$
$$\equiv x^{11} \equiv x$$

Wendet man also in den Cyklen von $\varphi(x)$ die Substitution $\varphi(x)$ abermals an, so erhält man wieder die Substitution x.

Wir suchen nun $\varphi(a\varphi(x) + b)$.

$(a\varphi(x) + b)^9 + 3(a\varphi(x) + b)^4$; statt $\varphi(x)$ kurz φ,

$= a^9\varphi^9 + 9a^3\varphi^8 b + 3a^7\varphi^7 b^2 + 7a^6\varphi^6 b^3 + 5a^5\varphi^5 b^4 + 5a^4\varphi^4 b^5 + 7a^3\varphi^3 b^6 + 3a^2\varphi^2 b^7 + 9a\varphi b^8 + b^9 + 3a^4\varphi^4 + a^2\varphi^3 b + 7a^2\varphi^2 b^2 + a\varphi b^3 + 3b^4$.

Bildet man die Potenzen von φ, so bekommt man folgende Kongruenzen:

$$\begin{aligned}
\varphi &= x^9 + 3x^4 \\
\varphi^2 &\equiv 10x^8 + 6x^3 \\
\varphi^3 &\equiv 6x^7 + 3x^2 \\
\varphi^4 &\equiv 10x + 4x^6 \\
\varphi^5 &\equiv x^5 \\
\varphi^6 &\equiv x^4 + 3x^9 \\
\varphi^7 &\equiv 6x^8 + 10x^3 \\
\varphi^8 &\equiv 6x^2 + 3x^7.
\end{aligned}$$

In φ^n und φ^{n+5} sind gleiche Potenzen vorhanden, doch die Koëfficienten vertauscht. Trägt man die erhaltenen Werte oben ein und berücksichtigt man noch, dass

$$a^9\varphi^9 + 3a^4\varphi^4 \equiv a^4(\varphi^9 + 3\varphi^4) \quad [a \text{ Rest}]$$
$$\equiv a^4 x$$

so ist unter der Bedingung, dass *a quadratischer Rest:*

$$(a\varphi + b)^9 + 3(a\varphi + b)^4 \equiv 9ab^8x^9 + 8a^2b^7x^8 + 9a^3b^6x^7$$
$$+ 9a^4b^5x^6 + 5a^5b^4x^5 + 10ab^3x^4 + 6a^2b^2x^3 + 2a^3bx^2 + a^4x$$
$$+ 5ab^8x^4 + 2a^2b^7x^3 + 10a^3b^6x^2 + 6a^4b^5x + 3b^4$$
$$\equiv 9ab^8\left(x^9 + \frac{7x^8}{a^8b^2} + \frac{x^6}{a^7b^3} + \frac{3x^5}{a^6b^4} + \frac{6x^4}{a^5b^5} + \frac{8x^3}{a^4b^6} + \frac{10x^2}{a^3b^7}\right.$$
$$\left. + \frac{5x}{a^2b^8} + \frac{6}{ab^9} + 3x^4 + \frac{2x^3}{a^9b} + \frac{6x^2}{a^8b^2} + \frac{8x}{a^7b^3} + \frac{4}{ab^4}\right) - \frac{9}{b}$$

$$\varphi(a\varphi(x) + b) \equiv 9ab^8\varphi\left(x + \frac{2}{a^4b}\right) + \frac{2}{b}\,[aR]$$

Eine analoge Rechnung führt bei mod 7 auf die Kongruenz:

$$\varphi(a\varphi(x) + b) \equiv 2ab^4\varphi\left(x - \frac{2}{a^2b}\right) - \frac{2}{b}\,[aR]$$

indem hier $\varphi(x) = -x^5 - 2x^2$ als Substitution 2. Ordnung zugrund gelegt ist.

Die obige Kongruenz macht nun im Verein mit $ax + b$ (aR) ein System von $5 \cdot 11 + 5 \cdot 11 \cdot 11 = 560$ conjugierten Formen aus. Der Index des Systems ist 60480.

Beispiel: $\varphi(4\varphi + 6)$ gibt mod 7 die Substitution $(062)(451)3 = T$, während $\varphi(4\varphi + 5)$ die $(031)(264)5 = S$ liefert.

Bildet man $ST = (034)(165)2$, so entspricht dies der Form $\varphi(2\varphi + 5)$, welche ebenfalls dem System angehört.

Dabei ist $T = \varphi(4\varphi + 6) \equiv \varphi(x + 1) + 2$; $S = \varphi(4\varphi + 5) = 2\varphi(x + 4) + 1$ und endlich $ST = \varphi(2\varphi + 5) \equiv \varphi(x + 2) + 1$.

§ 10.

Die Permutationen.

Die Funktion $ax + b$ stellt bekanntlich $n(n-1)$ Permutationen von n Elementen dar, wobei a die Werte $1, 2, 3, \cdots n-1$ und b dieselben Werte und noch Null annehmen muss. Wir können uns nun die $n(n-1)$ Permutationen auch dadurch aus x verschaffen, dass wir zunächst die Substitution $n-1^{ter}$ Ordnung $\binom{ax}{x}$, statt x setzen, dann wieder und sofort, wodurch $n-1$ Substitutionen gewonnen werden. (a *ist Primitivwurzel von* n.) Hierauf setzen wir statt x die cyklische Substitution n^{ter} Ordnung $\binom{x+1}{x}$ ein, und zwar $n-1$ mal, so dass wir zu den obigen $n-1$ nochmals $(n-1)^2$ Substitutionen erhalten, im ganzen also $n(n-1)$.

Die Wiederholungen der Substitutionen $\binom{ax}{x}$ und $\binom{x+1}{x}$ nennen wir die erste, zweite etc. *Iteration mit* ax *oder* $x+1$.

Soll nun zu einer beliebigen Permutation jene Funktion gesucht werden, deren Restsystem mit der Permutation übereinstimmt, so kann man, falls „0“ nicht Anfangselement ist,

zunächst „0“ an die erste Stelle und die anderen Elemente in der gegebenen Reihenfolge dahintersetzen. Kennt man dann zu dieser Permutation die entsprechende Funktion, so ergibt sich aus dieser die zuerst gesuchte durch Iteration der Substitution $\binom{x+1}{x}$.

Dieses vorausgeschickt können wir zur Beantwortung der Frage übergehen, durch welche Substitutionsfunktionen kann man jede beliebige Permutation analytisch darstellen. Die direkte Lösung führt auf die *Lagrange*'sche *Interpolation,* einem Hilfsmittel, welches von Fall zu Fall angewendet werden muss, da kein Zusammenhang in den einzelnen Polynomen ersichtlich ist. Geht man dagegen von einer Reihe Funktionen *(conjugiertes System)* aus, so lassen sich schon allgemeine Regeln für die Bildung der Substitutionen aus Gruppen feststellen. Auf jedem Falle muss man aber zum Ziel gelangen, wenn man, wie es in den nächsten Paragraphen geschehen ist, diejenigen Funktionen bildet, welche nur *eine Transposition* bewirken und alle anderen Elemente festlassen. Jede Permutation geht aus x mittelst einer Reihe von Transpositionen hervor.

Die Zahl der aufzustellenden Funktionen ist, da Null immer, wie oben gesagt, Anfangsglied bleiben soll, die der Kombinationen zu je 2 aus n—1 Elementen, also $\binom{n-1}{2}$, was für mod 5, 7, 11 die Zahlen 6, 15, 45 ergibt. Es wird sich jedoch zeigen, dass diese Funktionen bezüglich 1, 3, 5 Fundamentalfunktionen entstammen, aus denen sie mit Hilfe der beiden cyklischen Substitutionen $\binom{x+1}{x}$ und $\binom{ax}{x}$ leicht abgeleitet werden können, und zwar so, dass ein einziges Polynom mit allgemeinen Koëffizienten zur Ableitung der speziellen Funktionen dient.

Gibt nämlich die Interpolation zunächst die Funktion f(x), so kann man dazu die einfache oder *Stammfunktion* suchen, aus welcher sie abgeleitet ist, durch „j“malige *Iteration* mit x + 1, wodurch das zweite Glied beseitigt, und durch „i“malige mit ax (a *Primitivwurzel von* n), wodurch der Koëffizient der höchsten Potenz zu „eins“ wird. Streicht man noch die Konstante, so hat man die reduzierte Form z. B. V.

Will man von V zu f zurückkehren, so wendet man zuerst „n—1—i“mal die Substitution ax an, fügt die Konstante „j“ dazu und iteriert dann mit $x + 1$ noch „n—j“mal. Die Zahlen n—1—i und n—j sind in den Tabellen als Indices den Funktionen beigefügt, wobei der Vollständigkeit wegen auch Null aufgenommen ist.

§ 11.

Die Permutationen von 5 und 7 Elementen.

Bei 5 Elementen liefert $U = x^3$*) alle Transpositionen, wie man aus der Tabelle ersieht und zwar braucht man nur x^3 und $4x^3$ mit $x + 1$ bezüglich 1,4 und 2,3mal zu iterieren.

Man hat:

	2	3	4
1	$U_{0,1}$	$U_{2,3}$	$U_{2,0}$
2		$U_{0,0}$	$U_{2,2}$
3			$U_{0,4}$ **)

Beispiel. Soll 23014 erhalten werden, so sucht man die Funktion mit dem Restsystem 01423, welche aus x durch die Transpositionen (24) (32) erhalten wird. Wir haben somit $U_{0,0} \cdot U_{2,2}$ d. h. $U_{2,2}$ ist auf $U_{0,0}$ anzuwenden. Nun ist $U_{2,2} = 4(x + 2)^3 + 3 = 4x^3 + 4x^2 + 3x$ in $U_{0,0}$ eingetragen:

$$(4x^3 + 4x^2 + 3x)^3 \equiv 3x^3 + 2x^2 + x$$

Restsystem 01423

Wird hierin noch 3mal $x + 1$ eingesetzt d. h. die 3. Iteration gemacht, so hat man 23014 · ———

Bei 7 Elementen erhält man durch die Interpolation 15 Funktionen, welche sich auf folgende 3 zurückführen lassen:

$$U = x^5 + 2x^3 + 5x$$
$$V = x^5 + 4x^3 + 6x$$
$$W = x^5 + x^3 + 3x$$

Diese 3 reduzierten Formen folgen aus $x^5 + ax^3 + 3a^2x$, wenn „a“ quadratischer Rest von 7.

*) Bekanntlich jene Funktion, welche *Hermite* zur Auflösung der Gleichungen 5. Grades mittels elliptischer Funktionen benützt hat.

**) Die Tabelle ist so zu verstehen, dass 1 mit 2 durch $U_{0,1}$, dagegen mit 3 durch $U_{2,3}$, mit 4 durch $U_{2,0}$ etc. tauscht.

Ist „a“ beliebig so hat man, wie im § 8 gesagt, alle 3gliedrigen formes réduites.

Die folgende Tabelle gibt wieder diejenigen Funktionen an, welche die einzelnen Transpositionen vollziehen und deren Produkte sonach sämtliche Permutationen liefern.

	2	3	4	5	6
1	$U_{0,2}$	$V_{2,5}$	$W_{4,1}$	$W_{4,4}$	$V_{2,0}$
2		$U_{0,1}$	$V_{2,4}$	$W_{4,0}$	$W_{4,3}$
3			$U_{0,0}$	$V_{2,3}$	$W_{4,6}$
4				$U_{0,6}$	$V_{2,2}$
5					$U_{0,5}$

Hierin ist $U_{0,0} = x^5 + 2x^3 + 5x$

$V_{2,0} = 4x^5 + 4x^3 + 5x$

$W_{4,0} = 2x^5 + x^3 + 5x$

$(U_0 + V_1 + W_4 \equiv x)$.

Bei der Substitution ax ist $a = 3$ zu nehmen.

Beispiel. $V_{2,3}$ soll nach Art von § 10 entwickelt werden.

V gibt 0465213, die Substitution 3x wird aus diesem

3x { I. It. 0536142, Cykl durch Übergehung von 2 Elemenmenten erhalten
II. It. 0623451,

+4 4360125, die 3. Iteration mit $x + 1$ verschiebt den Anfang um 3 Elemente, so dass 0125436 resultiert, was in Bezug auf 0123456 die Transposition (35) aufweist.

§ 12.

Die Permutationen von 11 Elementen.

Die Interpolation liefert nach § 4 die Funktion:

$f(x) = (1\xi_1 + 2\xi_2 + 3\xi_3 + 4\xi_4 + 5\xi_5 + 6\xi_6 + 7\xi_7 + 8\xi_8 + 9\xi_9 + 10\xi_{10})x^9$

$+(1\xi_1 + 4\xi_2 + 9\xi_3 + 5\xi_4 + 3\xi_5 + 3\xi_6 + 5\xi_7 + 9\xi_8 + 4\xi_9 + 1\xi_{10})x^8$

$+(1\ +8\ \ 5\ \ 9\ \ 4\ \ 7\ \ 2\ \ 6\ \ 3\ \ 10\ )x^7$

$+(1\ \ 5\ \ 4\ \ 3\ \ 9\ \ 9\ \ 3\ \ 4\ \ 5\ \ 1\ )x^6$

$+(1\ \ 10\ \ 1\ \ 1\ \ 1\ \ 10\ \ 10\ \ 10\ \ 1\ \ 10\ )x^5$

$+(1\ \ 9\ \ 3\ \ 4\ \ 5\ \ 5\ \ 4\ \ 3\ \ 9\ \ 1\ )x^4$

$+(1\ \ 7\ \ 9\ \ 5\ \ 3\ \ 8\ \ 6\ \ 2\ \ 4\ \ 10\ )x^3$

$+(1\ \ 3\ \ 5\ \ 9\ \ 4\ \ 4\ \ 9\ \ 5\ \ 3\ \ 1\ )x^2$

$+(1\ \ 6\ \ 4\ \ 3\ \ 9\ \ 2\ \ 8\ \ 7\ \ 5\ \ 10\ )x$

woraus sich die 45 Funktionen, entsprechend von $\frac{10 \cdot 9}{1 \cdot 2} = 45$ Transpositionen berechnen lassen. Werden die Funktionen nach § 10 behandelt, so bekommt man die reduzierten Formen:

$$S = x^9 + x^7 + x^5 + x^3 + 4x$$
$$T = x^9 + 5x^7 + 3x^5 + 4x^3 + 3x$$
$$U = x^9 + 4x^7 + 5x^5 + 9x^3 + x$$
$$V = x^9 + 9x^7 + 4x^5 + 3x^3 + 9x$$
$$W = x^9 + 3x^7 + 9x^5 + 5x^3 + 5x,$$

welche einer Grundform entstammen. Die letztere heisst:

$$R = x^9 + ax^7 + a^2x^5 + a^3x^3 + 4a^4x$$

wo a quadratischer Rest von 11 ist. Aus R ergeben sich rückwärts die Funktionen der folgenden Tabelle, deren Produkte die $11! = 39916800$ Permutationen von 11 Buchstaben analytisch darstellen.

	2	3	4	5	6	7	8	9	10
1	$W_{0,1}$	$V_{8,9}$	$U_{4,3}$	$T_{6,8}$	$S_{2,2}$	$S_{2,7}$	$T_{6,1}$	$W_{4,6}$	$V_{8,0}$
2		$W_{0,3}$	$V_{3,8}$	$U_{4,2}$	$T_{6,7}$	$S_{2,1}$	$S_{2,6}$	$T_{6,0}$	$U_{4,5}$
3			$W_{0,2}$	$V_{8,7}$	$U_{4,1}$	$T_{6,6}$	$S_{2,0}$	$S_{2,5}$	$T_{6,10}$
4				$W_{0,1}$	$V_{8,6}$	$U_{4,0}$	$T_{6,5}$	$S_{2,10}$	$S_{2,4}$
5					$W_{0,0}$	$V_{8,5}$	$U_{4,10}$	$T_{6,4}$	$S_{2,9}$
6						$W_{0,10}$	$V_{8,4}$	$U_{4,9}$	$T_{6,3}$
7							$W_{0,9}$	$V_{8,3}$	$U_{4,8}$
8								$W_{0,8}$	$V_{8,2}$
9									$W_{0,7}$

Hier ist:

$$W_{0,0} = x^9 + 3x^7 + 9x^5 + 5x^3 + 5x$$
$$V_{8,0} = 4x^9 + 4x^7 + 4x^5 + 4x^3 + 5x$$
$$U_{4,0} = 9x^9 + x^7 + 5x^5 + 3x^3 + 5x$$
$$T_{6,0} = 5x^9 + 9x^7 + 3x^5 + x^3 + 5x$$
$$S_{2,0} = 3x^9 + 5x^7 + x^5 + 9x^3 + 5x$$
$$(W + V + U + T + S = 3x).$$

Aus den 3 entworfenen Tabellen ersieht man, dass der 2. Index mehr Werte annimmt als der erste. In der letzten z. B. 9, wobei für W nur 5,6; für V 1,10 für U 4,7 T 2,9 und S 3,8 fehlt. Zugleich ist die Tabelle eine Kontrolle für

die Rechnung, denn in den zur Diagonale parallelen Reihen sind die ersten Indices gleichgross, während die zweiten die konstante Differenz 1 haben, so dass ein Fehler sofort zu erkennen wäre.

Ferner folgt aus der letzten Tafel, dass eine Transposition zwischen zwei ursprünglich benachbarten Elementen mit Hilfe der Funktion W vor sich geht, dagegen tritt V ein, wenn ein Element mit dem übernächsten tauscht, U, wenn 2 Elemente dazwischen liegen, T bei einem Intervall von 3, bei 4 und 5 Zwischenräumen kommt man auf S, bei 6 wieder auf T, dann weiter auf U und endlich zu V zurück.

Wenn ich hiemit meine Untersuchungen abbreche, so bin ich mir wohl bewusst, dass noch manche Frage einer späteren Beantwortung anheim gegeben ist, weshalb ich mit vorliegender Studie durchaus nicht den Anspruch auf vollständige Erschöpfung der schwierigen Materie erheben, vielmehr zu eingehenderer Behandlung derselben anregen will. Was insbesondere die Anwendung der Substitutionen zur Auflösung der höheren Gleichungen betrifft, so verweise ich auf die höchst interessanten Arbeiten von *Lagrange, Hermite* und *Galois.*

Nürnberg, im Juni 1885.